WHITE PAPER

Cybersecurity Essentials

The Critical Cybersecurity Tools Needed to Protect Corporate Networks, Devices & Data in an Increasingly Hostile & Complex World

portnox™

www.portnox.com

An Age of Cybersecurity Crisis

The 2020s are quickly being defined as a decade of globalism driven by digital connectivity, technological innovation and the questioning of socioeconomic norms that have persisted since the early 20th century.

If the 1970s gave rise to the "me" generation, the 2020s can only be described as the "now" generation. Information at unprecedented scale is available at our fingertips—anywhere, anytime, in nearly any format. This has changed the expectations of the average consumer and the military-industrial complex alike.

We communicate online, we work online, we wage war online.

In this new digitally connected age, data has become the world's most valuable resource. Data means power. Those that hold it have the edge. This applies to individuals, businesses and governments alike. With data at such a premium, it's no wonder a market for data theft has flourished — after all, it's human nature. For every good deed, a bad deed lays in wait.

The hacker represents the modern day boogie man — lurking out in the digital ether, unseen ... but we know he's there. It's a delicate balance, especially at the corporate level. Companies play digital defense because they possess the data, whether it be financial, legal, personal or otherwise.

Hackers innovate, finding new ways into corporate networks, devices and applications. This continuum has in turn created the cyber security market, where vendors strive to make a quick buck by plugging the latest hole in corporate infrastructure. But it's been a losing battle thus far because security solutions that come to market are reactionary to problems their customers are already facing. The black hats have the element of surprise, and companies typically don't know what hit them until it's too late.

This new digital dystopia is here to stay. And while it might make you want to shield your eyes like an episode of *Black Mirror*, the outlook for data protection and cyber security is not as bleak as it may seem. The first step to resolution (or general improvement), is to acknowledge cyber security challenges and shortcomings, and begin to pave a path forward.

More Endpoints, More Complexity, More Threats

Today, corporate networks are expanding and evolving in true Darwinistic fashion thanks to architectural advancements, new networking protocol standards, device proliferation, hybrid work policies.

You could write a dissertation on this topic alone. The point is: the corporate network now extends to wherever authorized devices can connect to gain access to company resources.

All of this proprietary, confidential or merely sensitive data being accessed across these parts of the network is no longer safe behind your castle walls. The physical headquarters still exists, but it's basically just a "fat" branch like any other satellite office or employee working from home.

The number of significant cyberattacks globally is increasing and includes devastating ransomware attacks that are breaching even the most secure networks. But are we really surprised? Cyber defense (and offense) is the national security priority for every developed country on Earth. We'll never know the global investment made into clandestine black hat innovation for the sole purpose of destabilizing the digital footprints of nations perceived to be threats. We may not want to.

Ignorance here really can be bliss.

The Bad News

31%+ There were on average **270 attacks per company over the year**, a 31% increase over 2020. Third-party risk continues to dominate: successful breaches to the organization through the supply chain have increased from 44% to 61%. *(Accenture)*

$5.3M As they've adopted these new extortion approaches, ransomware gangs have become greedier. **The average ransom demand was $5.3 million.** That's up 518% from the 2020 average of $847,000. *(Palo Alto)*

32% Nearly a third of organizations say **security is not part of the cloud discussion** from the outset and they're trying to catch up. *(Accenture)*

The Good News

82% Say their budgets have increased in the last year. **IT security budgets are now up to 15% of all IT spending**, 5 percentage points higher than reported in 2020. *(Accenture)*

49% IT executives said their **top security priority is the protection of sensitive data**. *(IDG)*

2x The global median dwell time — the duration between the start of a security intrusion and when it's identified — has dropped to below a month for the first time, standing at 24 days in 2021. That means **incidents are being identified twice as quickly as they were year-over-year**. *(ZDNet)*

The Saturated Cybersecurity Vendor Landscape

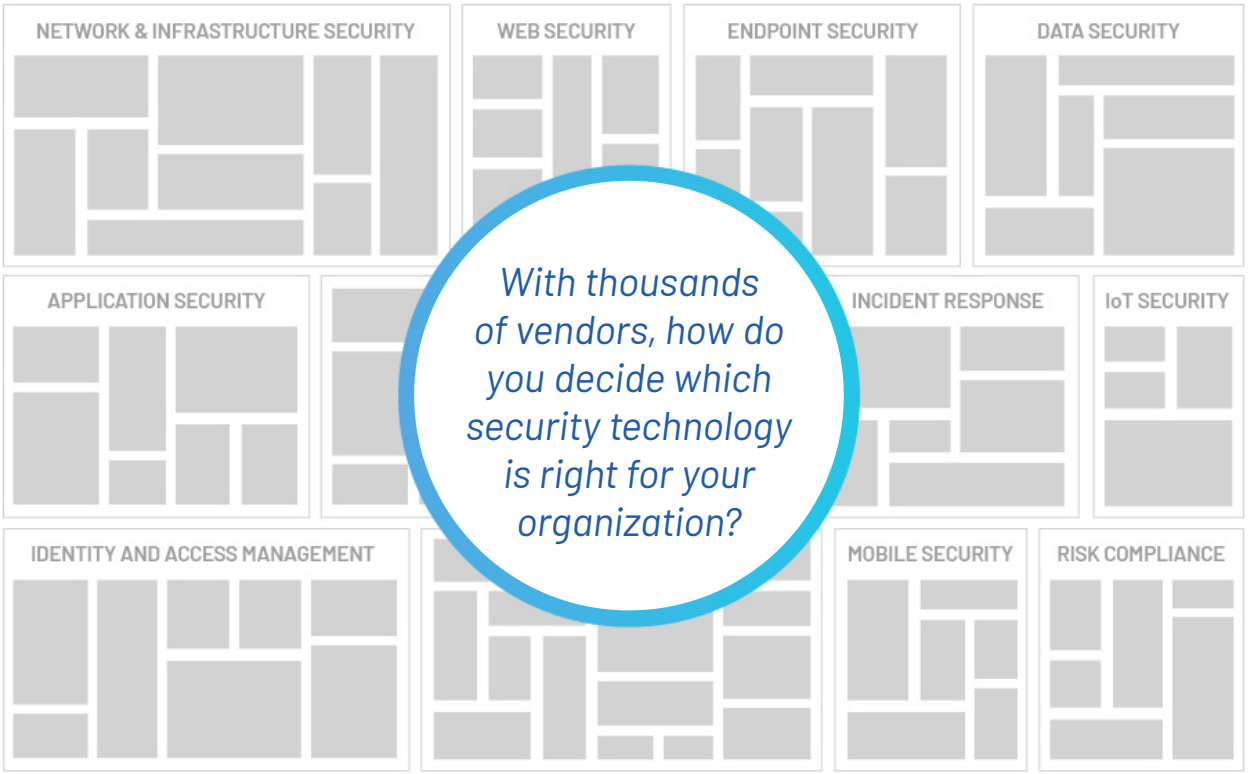
The problem is that these malicious and invasive cyber tactics are being leveraged in the private sector. That's where the real money lives after all.

As the variety and severity of these cyber attacks on businesses expand and intensify, the cyber security vendor landscape grows ever more saturated.

This vendor saturation isn't deliberate, but it does create a FOMO mentality among IT security administrators — *oh god, am I at risk if I don't have a tool for this or for that?!*

No one wants to be the next big headline, but at the same time there's no clear and obvious guide for what to invest your meager IT security budget in.

Cyber security is a market plagued by acronyms, especially on the networking side. This doesn't simplify matters. The real problem is that the security technology landscape, like its lingo, is too complex.



How can anyone with their back against the wall make sense of the options presented to them in this Cyberscape? The reality is that we need to get back to basics. What businesses large and small need to be asking is: what's essential to maintain business continuity safely and securely?

Key Areas in Cybersecurity Today

Don't let the Cyberscape fool you. When it all boils down, cyber security can be fundamentally bucketed into three areas:

1. Network Security
2. Endpoint Security
3. Application Security

While security software vendors have made the subcategorization of these areas into a cottage industry, this overarching security trilogy is pretty straightforward. In essence, companies should seek to secure their networks, the devices in use across those networks, and the business applications in use across those devices.

Network Security

Simply put, network security is a set of rules and configurations designed to protect computer networks and the data in transit across them via software and hardware.

Organizations large and small require a degree of network security to protect it from the proliferation of cyber threats we covered earlier.

Network security typically consists of three different controls: physical, technical and administrative. Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, wiring closets and so on.

Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold: it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees, contractors and guests on the network.

Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how the IT department can implement changes to the infrastructure.

Endpoint Security

Endpoint security is the practice of protecting enterprise networks against threats originating from on-premises or remote devices. An endpoint is any device that provides an entry point to corporate assets and applications and represents a potential cybersecurity vulnerability. Examples include desktops, laptops, servers, workstations, smartphones and tablets.

Historically, most organizations have relied on tools such as firewalls, VPNs, and antivirus programs to safeguard sensitive information, prevent unauthorized access to critical applications and IT systems, and protect against malicious software and other vulnerabilities.

As we've touched on, however, companies are increasingly adopting mobile applications and cloud services that erode the once well-defined enterprise network perimeter. Many enterprises are now taking a defense-in-depth approach to endpoint protection, instituting a wider range of security controls to protect against a broader array of threats.

Application Security

Application security is the discipline of processes, tools and practices aiming to protect applications from threats — both internal and external to an organization. Cyber threat actos exploit vulnerabilities in enterprise applications to capture data, intellectual property, and more — often with impunity. Application security can help organizations protect all kinds of applications (such as legacy, desktop, web, mobile, etc.) used by corporate stakeholders including customers, business partners and employees.

Most successful breaches target vulnerabilities that reside in the application layer, such as the recent log4j vulnerability. As a result, IT teams must be extra vigilant about application security.

To further compound the problem, the number and complexity of applications is growing, as is the number of devices and device types running them.

An Age of Cybersecurity Crisis

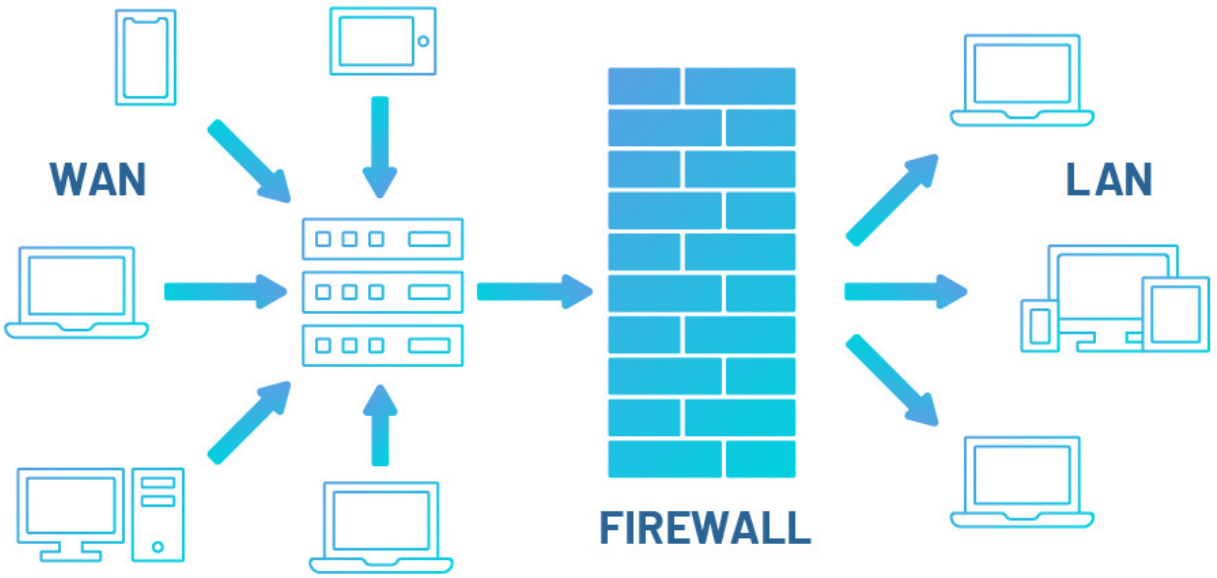
Cybersecurity Essential #1: Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for decades. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks. Next-generation firewalls are more sophisticated than packet-filtering and stateful inspection firewalls. Why? They have more levels of security, going beyond standard packet-filtering to inspect a packet in its entirety. That means inspecting not just the packet header, but also a packet's contents and source. NGFW are able to block more sophisticated and evolving security threats like advanced malware.

Necessary capabilities:

- Advanced Threat Protection — Most traditional firewalls integrate with a separate intrusion prevention system (IPS) to gain additional security features. Next generation firewalls have IPS capabilities built in to protect against a wide variety of threats, such as DDoS attacks, malware and spyware. Further integration with threat intelligence systems like SIEM provide advanced layers of protection to defend against the modern threat landscape.
- SSL Inspection — Malicious threats can be hidden within encrypted web traffic. In order to filter out malicious content, the NGFW intercepts encrypted web activity to filter out malicious activity through a "man in the middle" approach. The NGFW will first decrypt the incoming web traffic

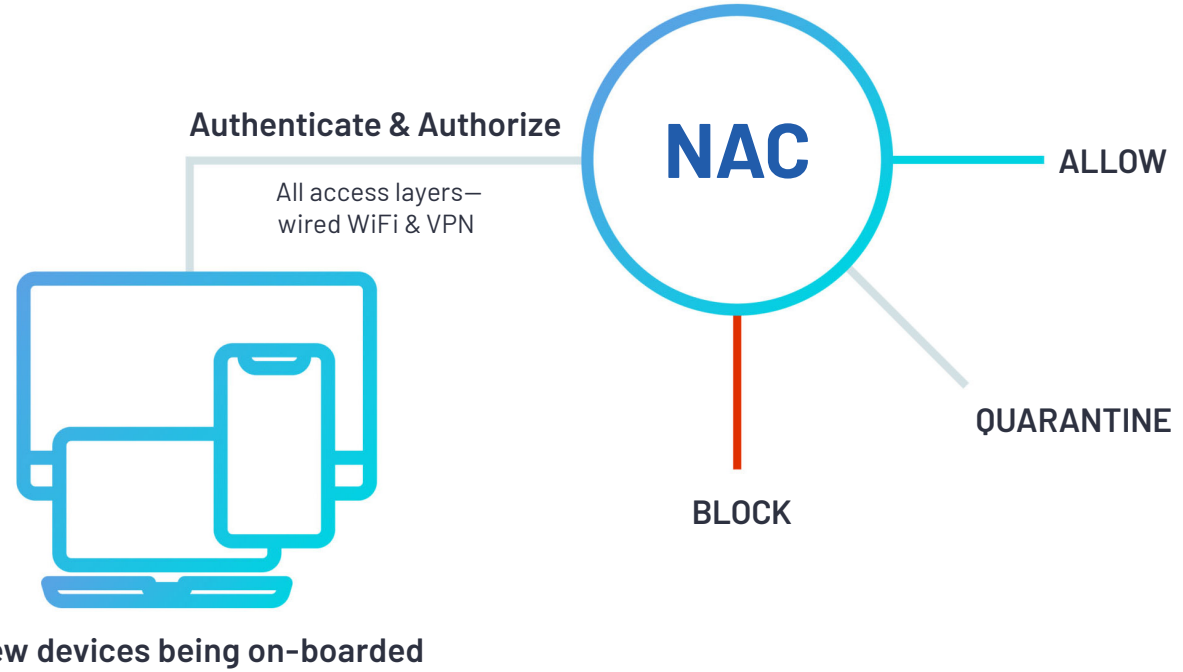


and then scan for threats like malware or viruses. After its examination, the traffic will be encrypted and forwarded to the user so that the user can access the data as originally intended.

- Application Control — The users on your network use several tools on their devices, such as email, social media and other vendor applications. Some of these web applications can be malicious and lead to open backdoors that can be exploited to enter your network. Application control allows organizations to create policies that either allow, deny or restrict access to applications. This not only protects organizations by blocking risky applications but also helps them manage their application traffic to ensure availability for business-critical resources.
- User Identity Awareness — User identity awareness allows organizations to enforce policies that govern access to applications and other online resources to specific groups or individuals. The NGFW integrates with your authentication protocols (such as LDAP or Active Directory) so that access is governed by user identity as opposed to IP address. User identity awareness not only helps organizations control the types of traffic allowed to enter and exit their network but also manage their users.
- Deep Packet Inspection — Deep packet inspection inspects data to identify and filter out malware and unwanted traffic. By inspecting the content of a data packet, the NGFW can intelligently determine which applications are being used or the type of data being transmitted. This allows the firewall to block advanced network threats (such as DDoS attacks, trojans, spyware and SQL injections) and evasion techniques used by threat actors.
- Centralized Management — Firewalls need proper security management to ensure that they meet the security needs of the organizations that need protection. Firewall capabilities need to be updated and firewall rules need to ensure they

are being properly enforced. Centralized management of your firewall(s) is crucial in gaining on overall view of your firewall configurations. Organizations need to ensure they can scale their firewall to ensure that their organization has maximum protection to fit their growth needs.

- Reporting & Insights — Firewalls generate logs that detail information about security and network traffic that security administrators review to understand the overall activity. This information provides organizations with useful insights to help them prioritize application traffic and understand their network security and monitor user activity.



Cybersecurity Essential #2: Network Access Control (NAC)

NAC is a technology that enables organizations to enact its own unique policy for how and when endpoints (desktops, laptops, smartphones, etc.) can connect to their corporate networks. NAC solutions are typically designed to allow IT security teams to gain visibility of each device trying to access its network, and specifically the type of device and access layer being used (i.e. wifi, wired ports, or VPN).

Today, NAC provides a number of powerful features on top of what it was originally designed for years ago. These include security posture assessments for endpoints, which pinpoints any associated endpoint risks, allowing network security administrators to control network access based on their organization's risk tolerance threshold.

With the rise of cloud computing, remote workforces, bring-your-own-device (BYOD)

policies, and the internet of things (IoT), network access control has become a much more critical part of the larger cybersecurity technology stack at most companies. The technology itself has also evolved quite drastically in response to these emerging trends and their impact on networking and ensuring network security.

Necessary capabilities:

- Network Visibility & Device Discovery — A NAC solution discovers and identifies all devices/users in the network before they are granted network access, requiring continuous monitoring of the network and devices connected to it. The system enables the discovery, classification and assessment of every device connected to the network. Configuration and security state of every device is monitored, ensuring that the network and devices are compliant to the organizational security policy.
- Full Access Layer Coverage — As today's networks explode in size and scope, particularly with remote workforces on the rise, it's imperative that your NAC solution can manage access control across all existing access layers. This includes the obvious – wired ports and WiFi. It also must be able to manage the various remote access methods used within your organization. These may include VPN, Teleworker Gateways, and beyond.
- Authentication Services — Traditionally, enterprises have enabled network authentication via usernames and passwords. As we now know today, this method of authentication can be easily compromised by bad actors, making it no longer sufficiently secure for enforcing network access control. Any NAC worth its salt should offer several methods for authentication, including: role-based, MAC authentication bypass (MAB), and certificate authority.
- Device On-Boarding — Business units and even departments (think Finance & Accounting, for example) often have their own VLANs since they're dealing with very sensitive, confidential data. The task of setting up such VLANs and onboarding new devices is just one of dozens of tasks overseen by frequently overburdened IT teams. So, if not done correctly at first, it can open the door to potential network vulnerabilities, such as a person gaining access to a part of the network he/she should not have the privileges for. At a small scale, managing access manually is often sufficient. For larger organizations, however, this just isn't sustainable. As a result, many large organizations that don't have a secure onboarding process will often compromise on network security hygiene.
- Policy Configuration — Network security teams define and activate access control policies to control device access to the corporate network, which is ultimately based on the device authorization state. Once a device is authorized for network access, a network access policy determines which specific virtual LAN (VLAN) that device or user is directed to. On top of that, the policy also defines, for each type of authorization violation, whether to deny entry or whether to quarantine the device by assigning it to a specific VLAN or apply an access control list (ACL).

- Endpoint Risk Monitoring — Your corporate network is only as strong as its weakest security link. This means continuous risk posture assessment is paramount. By continually monitoring the network, your network and security teams can stay ahead of cyberattacks with the ability to identify new risks in real-time, react to these risks, and take action. In a world with ever-expanding boundaries and an exponential increase in types of endpoints, continuous risk posture assessment must function no matter location, device type, or the type of data being transferred.
- Device Remediation — Having a rapid remediation plan in place will not only help prevent further damage or the lateral spread of attacks but also allow for business continuity.

  Effective endpoint remediation consists of:

  - Automated Patch Updates Across the Network — Enforce necessary patch, anti-virus, operating system, and application updates across managed and unmanaged endpoints.
  - Immediate Incident Response – Contain ransomware events by remotely dis-connecting endpoints from the network without the need for manual intervention.
  - Armed Incident Response Teams — Arm IT professionals and network admins with the ability to remotely take actions on employees' devices. The proliferation of IoT devices over the last decade has prompted a growing number of network security concerns. With all of these devices – printers, CCTV cameras, ATMs, MRI machines, etc. – now connected to their respective networks, it's exponentially expanding corporate threat surfaces.
- Compliance Enforcement — NAC is used to enforce regulatory policies and maintain compliance across the organization. In practice, this typically means:
  - Understanding how mobile, BYOD, and IoT devices will affect and transform not only the organization but the industry and implementing the right processes and tools control them.
  - Tracking any network related device or program in real-time via a centrally secured platform providing full and actionable visibility.
  - Controlling access to the network and to cloud applications, even based on the geographical locations of users.
  - Ensuring that the business is in compliance with governmental regulations like SOX, PCI DSS, HIPPA, FINRA, FISMA, GLBA among others. Strict compliance will provide legitimacy with clients and partners.

Cybersecurity Essential #3: Antivirus

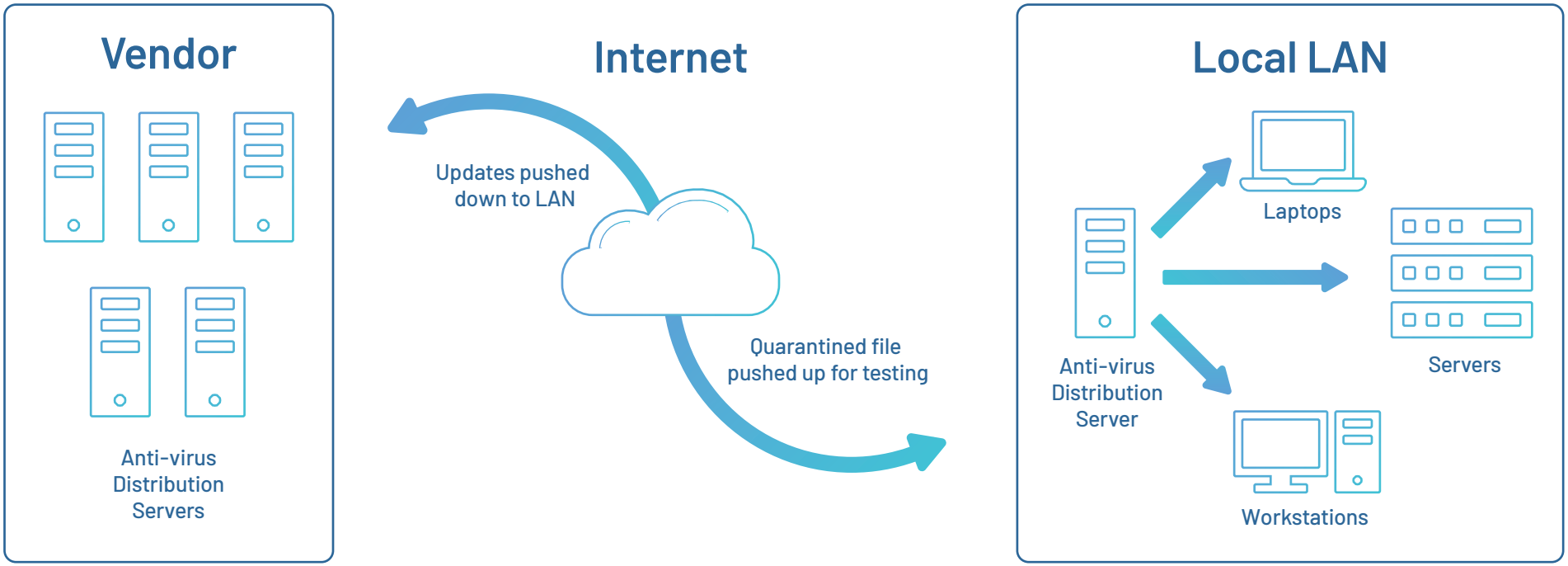
Antivirus software helps protect computers against malware and cybercriminals. Antivirus software looks at data – web pages, files, soft-ware, applications - traveling over the network to your devices. It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior. It seeks to block or remove malware as quickly as possible.

Antivirus protection is essential, given the array of constantly-emerging cyber threats. If you don't have protective software installed,

you could be at risk of picking up a virus or being targeted by other malicious software that can remain undetected and wreak havoc on your computer and mobile devices.

Necessary capabilities:

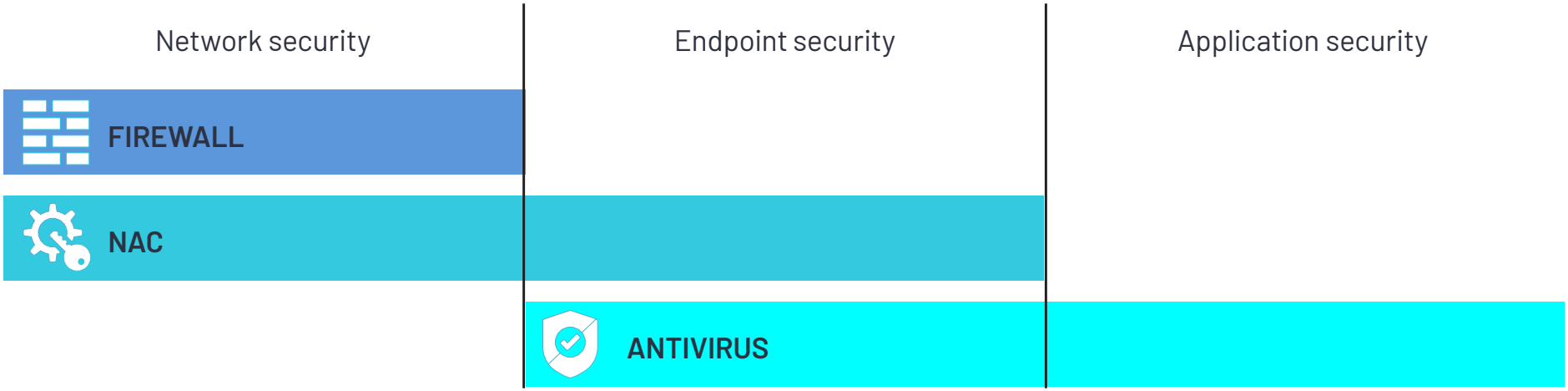
- Real-time Scanning — While all antivirus software is specifically designed to detect the presence of malware, not all of them detect in the same way. Ineffective products force you to run a manual scan to determine if any systems have been affected, while the best forms of software have dynamic scanning features that are repeatedly checking your computer for the presence of malicious entities. Without this feature, it's much easier for something to infiltrate a device and begin causing damage before you even realize it.
- Automatic Updates — Updates are vital for all forms of software, but this is especially true when it comes to antivirus. Because new types of malware are constantly being developed, antivirus software needs frequent updates in order to track and contain new threats that didn't even exist when it was first installed. If you have to install updates manually, you might miss important new protections



and expose your system to infection, so always make sure your antivirus software is capable of installing updates automatically and frequently.

- Protection for Multiple Apps — Threats exist across the entire spectrum of applications and services that you rely on for your everyday tasks. From email clients, to your CRM, ERP, and beyond, harmful software can sneak into systems from a variety of different sources. Antivirus programs need to protect multiple vulnerable applications from potential dangers.
- Auto-Clean — If the antivirus software immediately detects malicious software, why wouldn't it delete the code on the spot? Unfortunately, some solutions simply place the malware in a quarantine zone upon detection, waiting for the user to log on and manually delete it. You should choose a program that utilizes an auto-clean feature to rid itself of viruses.
- Fights Against All Types of Malware — Between trojans, bots, spyware, viruses, etc., there are many different types of malware that can harm your computer, and antivirus programs are sometimes designed only to target a specific type of software. It's better to go with a program that can comprehensively detect all forms of malware.

Essential Cyber Security Coverage

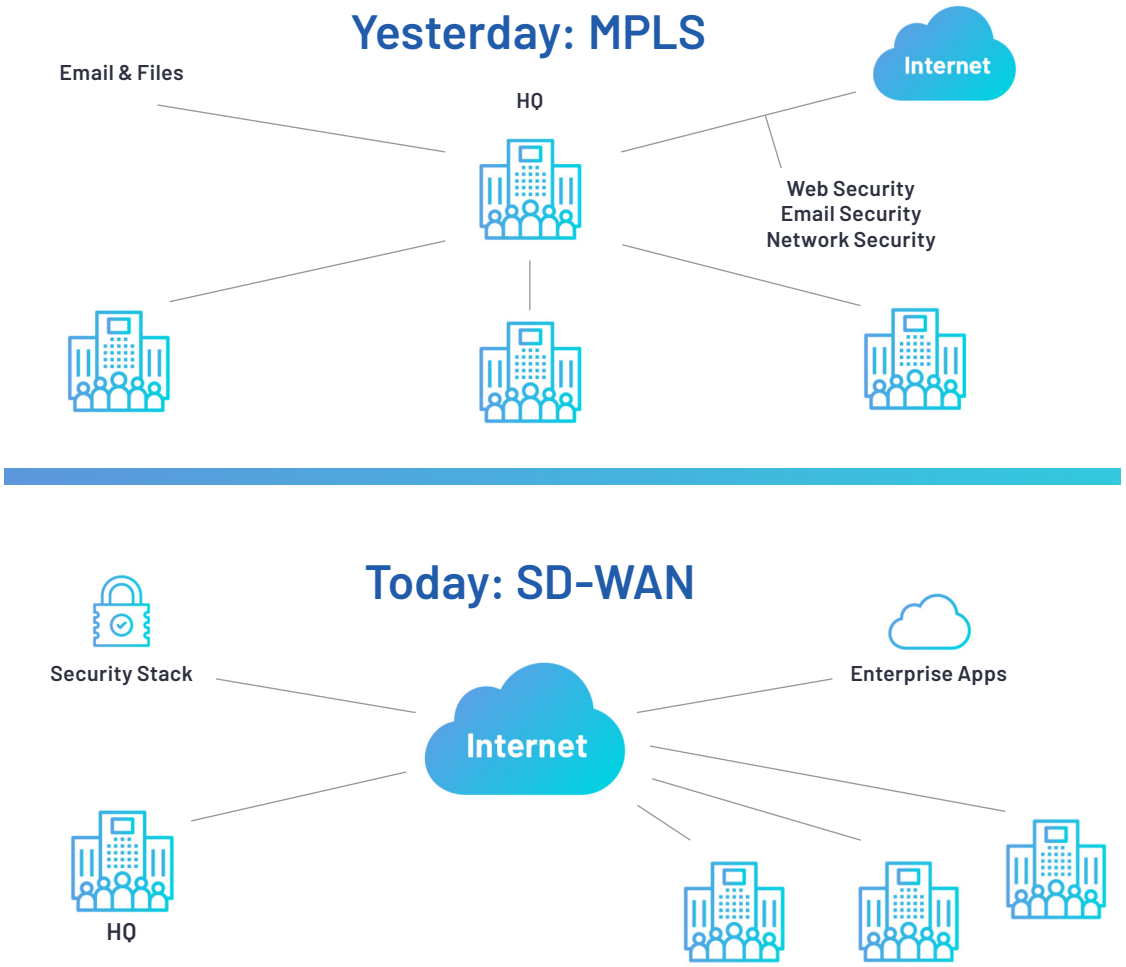


Future-Proofing Your Cybersecurity Program

Networking Innovation

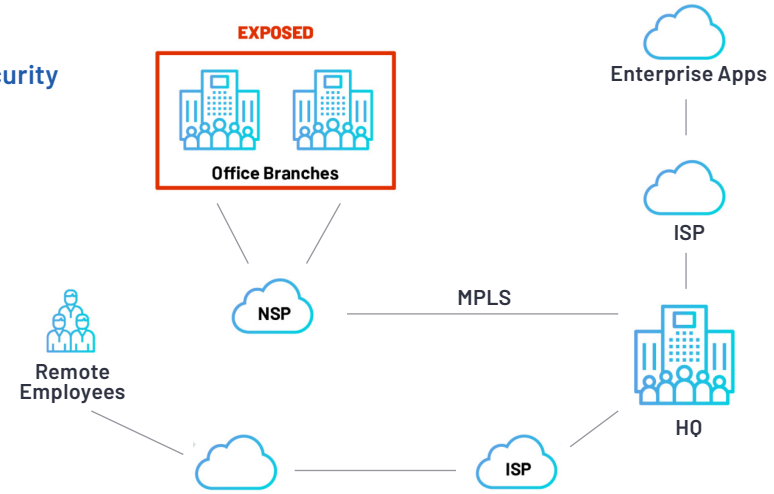
The adoption of Software-as-a-Service (SaaS) and cloud services has decentralized data traffic flows, making Multiprotocol Label Switching (MPLS) inefficient for wide area network (WAN) transport. This has given rise to SD-WAN for the implementation of software-defined branch (SD-branch), now allowing IT environments to be extended to branches outside of the headquarters that need high-quality network connectivity.

Traditionally, in order for most cyber security products to effectively operate, they needed a direct connection to headquarters and appliances deployed on-site at individual branches. This is a costly, time-consuming endeavor, and has historically limited the use of SD-WAN and SD-branch. Fortunately, SaaS is eliminating the need for on-site appliances and ongoing maintenance. Now, all one needs is an internet connection to implement.



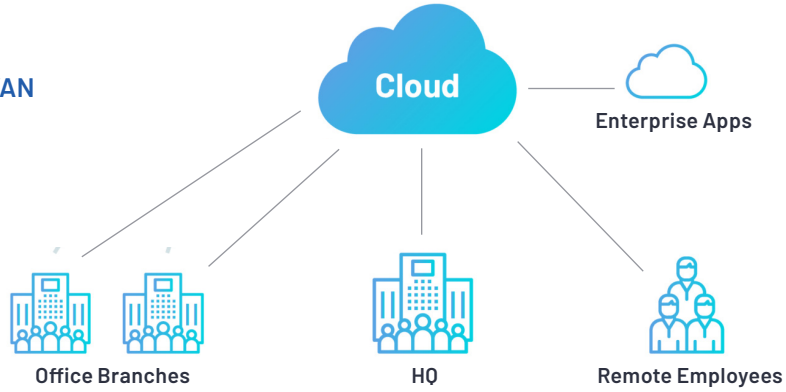
Yesterday

Traditional Network Security Architecture



Today

SASE Architecture/SD-WAN



The Convergence of Networking & Security

In 2019, Gartner introduced SASE as a new enterprise networking technology category. In essence, SASE converges the functions of network and security solutions into a single, unified cloud service.

This marks an architectural transformation within the realm of enterprise networking and security, and it means that IT teams can now deliver a holistic and flexible service to their businesses.

The logical next step in the evolution of cyber security is for organizations to be able to leverage security solutions that are delivered as a cloud service. This eliminates the need for costly on-site appliances and on-going maintenance.

About Portnox

Portnox offers cloud-native network and endpoint security essentials that enable agile, resource-constrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of enterprise networks, the proliferation of connected device types, and the increased sophistication of cyberattacks.

portnox™

For more information, please visit www.portnox.com.